FINANCIAL INSTITUTIONS TODAY

News and topics of interest to financial institutions regulated by the Department of Banking and Finance

April 2017

Inside this issue:

Governor Deal signs House Bill 143

Governor Deal signed House Bill 143 into law on May 1, 2017, and it will go into effect on June 1, 2017. The bill was introduced by Representative Bruce Williamson at the request of the Department of Banking and Finance (Department) and sponsored in the Senate by Senator John Kennedy. The bill revises statutory provisions governing most of the entities regulated by the Department – banks, credit unions, trust companies, bank holding companies, money service businesses, and mortgage lenders and brokers – as well as certain provisions addressing the Department's general powers.

Among other items, the bill:

1) empowers the Department to issue stand-alone trust company charters;
2) permits all trust companies that are chartered out of state to act as a fiduciary in Georgia;
3) streamlines the legal lending limit calculation for banks;
4) authorizes the imposition of convenience fees for the handling of electronic payments;
5) clarifies the Department's ability to examine and regulate third-party service providers;
6) modifies the age at which a minor can open a bank account only in his or her name;
7) confirms that state-chartered institutions can conduct business on Sunday;
8) limits the ability of credit unions to accept uninsured deposits;
9) provides parity with federal credit unions by including employment within a geographic field of membership;
10) eliminates the requirement that the Department approve all fixed asset investments by credit unions;
11) enables credit unions to purchase whole loans from a financial institution; and
12) increases the required bond amount for mortgage brokers and mortgage lenders.

House Bill 143 can be viewed at: https://gov.georgia.gov/sites/gov.georgia.gov/files/related_files/document/HB%20143%202017.pdf. The Department strongly encourages every regulated entity to review the bill to ensure a thorough understanding of all the applicable revisions.

The Department will issue proposed rules and regulations in May to, among other items, implement some of the statutory changes contained in House Bill 143.

Georgia Bankers' Input Needed on 2017 National Survey

State bank supervisors in coordination with the Federal Reserve are planning the fifth annual Community Banking in the 21st Century research and policy conference in St. Louis, Missouri. The goal of the conference is to provide a venue for and encourage research on community banking. This research is a critical component to improving public policy as it relates to community banks and local communities.

For last year's conference, state regulators conducted a nationwide survey of community banks with over 550 banks participating in this valuable survey. The results of the National Survey and the commissioner-to-banker outreach meetings are highlighted in a publication released during the conference. The 2016 report can be downloaded here.

The National Survey for 2017 is available at https://sri.cornell.edu/CB21/2017/ and takes approximately 20 minutes to complete. The purpose of the survey is to give researchers and policy makers an opportunity to hear directly from community banks on a range of important topics. The Department strongly encourages our Georgia community bankers to participate in this survey and provide feedback on the many important issues currently facing Georgia banks.

Preventing Financial Exploitation of Elders

New Community Resources

The Federal Deposit Insurance Corporation (FDIC) has made enhancements to its *Money Smart for Older Adults* curriculum that provides new information and resources to help older adults and their caregivers avoid financial exploitation through fraud and scams.

Money Smart for Older Adults identifies common types of elder financial exploitation, such as imposter scams and identity theft, and is designed to inform adults age 62 or older and their caregivers about ways to prevent, identify, and respond to financial exploitation. Also included is information on how older adults can plan for a secure financial future and make informed financial decisions.

Money Smart for Older Adults was developed jointly by the FDIC and the Consumer Financial Protection Bureau (CFPB) in response to the financial exploitation of senior citizens - an abuse that is rarely reported. According to the National Adult Protective Services Association, only one in 44 cases of financial abuse comes to the attention of authorities, and 90 percent of victims are exploited by a relative, friend, or trusted acquaintance.

Money Smart for Older Adults is a stand-alone, instructor-led training module designed to be delivered by trusted individuals who serve the older adult population. Instructors often include representatives of social service agencies, law enforcement, and financial institutions, as well as legal professionals and other volunteers.

The three-part module consists of an instructor guide, a resource guide, and a PowerPoint presentation that supplements classroom instruction. Materials are available in English and Spanish. The curriculum, the resource guide available from the CFPB, and success stories about the *Money Smart* curriculum can be found on the FDIC website.

Mandated Reporters of Elder Abuse in Georgia

In Georgia, elder persons, as defined by the Official Code of Georgia Annotated (O.C.G.A.) § 30-5-3, are protected from abuse, including financial exploitation. Various local and state law enforcement agencies work closely with Adult Protective Services to address cases of financial exploitation of vulnerable adults. In Georgia, elder abuse is a felony under O.C.G.A. § 16-5-102.

Pursuant to O.C.G.A. § 30-5-4, employees of financial institutions are considered “mandated reporters” of suspected financial exploitation unless acting as a fiduciary, as defined in O.C.G.A. § 7-1-4, but only for such assets that the employee is holding or managing in a fiduciary capacity. It is the understanding of the Department that those employees acting in a fiduciary capacity were exempted because their fiduciary responsibilities would require a standard of conduct at least equal to that set forth in O.C.G.A. § 30-5-4. Mandated reporters who knowingly and willfully fail to report a case of elder person abuse may be charged with a misdemeanor. Directors and management teams may be concerned with the possible violation of privacy laws, but interagency guidance (noted below) provides safe harbor.

Financial Crimes Enforcement Network

Further, in certain circumstances involving suspected elder abuse, the institution should submit a Suspicious Activity Report to the Financial Crimes Enforcement Network. In general, a report is required on transactions aggregating $5,000 or more, conducted or attempted by, at, or through the institution or an affiliate, if the institution or affiliate knows, suspects, or has reason to suspect such transactions may involve illegal activity. Refer to federal guidance (noted below) for other relevant details. The Department receives copies of Suspicious Activity Reports meeting certain criteria outlined in Department Rule 80-9-1-.02 Suspicious Activities.

Select Other Laws, Regulations, and Regulatory Guidance

- FIN – 2011– A003: Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation
- Interagency Guidance on Privacy Laws Reporting Financial Abuse of Older Adults
- NCUA Letter to Credit Unions No. 13-CU-08: Reporting Elder Abuse or Financial Exploitation
- http://aging.dhs.georgia.gov.

Cybersecurity: Ransomware

Ransomware is malicious software that encrypts computer files, making files or the operating system inaccessible to intended users. The files are encrypted by hackers to make the user pay a ransom for access. Hackers take advantage of vulnerabilities – both social and technical – to deploy the ransomware. Prompt action to combat an intrusion is crucial to reducing the risk to your institution. Educating staff is key to prevention.

Methods of Deployment

Social scams continue to provide unintended access. Phishing email scams are the most commonly used method of hacking into systems and can be preventable with appropriate training. Also, employees should be aware that surfing the internet to take advantage of free downloads and access compromised websites may compromise security. The employees may not realize that their active participation could inadvertently provide access to their computer, the institution's network, and other connected devices. Technical vulnerabilities continue to undermine security. Out-of-date software can create unintended entry points. The software's end of life may have arrived and the software may no longer be supported by the vendor, leaving no watchdog for new or not-yet-identified vulnerabilities; or, the software patches available for vendor-supported software may be unapplied by the institution's busy staff, leaving known weaknesses unaddressed. An institution should have policies that require oversight of software vendors for information regarding end of life and patch updates as a part of its vendor management program.

Next Steps if Ransomware is Suspected

Typically, the first thing an employee should do if ransomware is suspected to have been encountered is to unplug the computer from the network and turn off the wireless connection to minimize the spread of ransomware to other machines. After the network connection has been shutdown, notify your institution's IT department immediately. Your IT Department may have another plan, so you should confirm the protocol at your institution.

Prevention Tips

Handle all technology resources with security in mind. The following are examples of ways to improve data protection as well as data integrity:

- Make sure anti-virus software and firewall definitions are up-to-date;
- Educate staff about ransomware and protocol;
- Use email encryption when sending sensitive data outside your organization;
- Only use devices approved in your policies for work;
- Do not send institution email to your personal email account;
- Lock your computer before stepping away from it;
- Take care to dispose of information on USB, CD's, or printed paper with sensitive data when no longer needed; and
- Refrain from discussing your institution's business with friends, family, or others.

Business Continuity Plans

Business continuity planning includes an effective risk assessment that identifies hazards and vulnerabilities, including technology specific threats like ransomware. Business continuity packages from vendors may be presented with each of your systems available in real time, which may result in some sticker shock. Understanding time criticality and matching those requirements to recovery time objectives may result in a workable plan at a more affordable price. A continuity plan should include a timeline that identifies which systems are needed in real time through which systems are appropriate for delayed reinstatement (if any).

Breach of Customer/Member Information – Regulatory Requirements

The Interagency Guidelines Establishing Information Security Standards set forth standards pursuant to Section 39 of the Federal Deposit Insurance Act, 12 U.S.C. 1831p--1, and sections 501 and 505(b), 15 U.S.C. 6801 and 6805(b), of the Gramm-Leach-Bliley Act (GBLA). Appendix A to Part 748 of the National Credit Union Administration Rules and Regulations makes GBLA applicable to credit unions. If the institution has determined that sensitive customer/member information has been breached, then those customers/members must be notified. Sensitive information has been defined as name, address, or telephone number in conjunction with a social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Consult your federal regulator for more information. O.C.G.A. § 10-1-910, § 10-1-911, and § 10-1-912 also have requirements in the event of security breaches.

Action on Applications for the Month

The following is a summary of official action taken on applications by state financial institutions under Title 7, Chapter 1 of the O.C.G.A. and petitions for certificate of incorporation of financial institutions and other matters of interest during the month of April 2017:

APPLICATIONS FOR NEW FINANCIAL INSTITUTION

FINANCIAL INSTITUTION	CAPITALIZATION	APPROVAL DATE	BEGIN BUSINESS DATE
Pacific Metro Bank 11625 Medlock Bridge Road Johns Creek, GA 30097 Fulton County	$ 12,000,000	Withdrawn 04-10-2017	

APPLICATIONS TO ESTABLISH A BRANCH OFFICE

FINANCIAL INSTITUTION	BRANCH OFFICE	APPROVAL DATE	BEGIN BUSINESS DATE
Members United Credit Union Albany	Leesburg 1148-1152 US 19 South Leesburg, GA 31763 Lee County	04-19-2017	
SunTrust Bank Atlanta	Fox Mill Centre 6723 Fox Centre Parkway Gloucester, VA 23061 Gloucester County	04-10-2017	
First Bank Dalton	Calhoun 197 W.C. Bryant Parkway Calhoun, GA 30701 Gordon County	08-02-2016	04-03-2017
Metro City Bank Doraville	Main Office 5114 Buford Highway Doraville, GA 30340 DeKalb County	04-11-2017	
Metro City Bank Doraville	Marietta 4273 Roswell Road Marietta, GA 30062 Cobb County	04-11-2017	

APPLICATIONS TO CHANGE LOCATION

FINANCIAL INSTITUTION	CHANGE LOCATION OF	APPROVAL DATE	EFFECTIVE DATE
SunTrust Bank Atlanta	West End From: 1715 West End Avenue Nashville, TN 37203 Davidson County To: 210 21st Avenue South Nashville, TN 37203 Davidson County	04-04-2017	

NOTICE OF CHANGE IN NAME

PREVIOUS NAME	NEW NAME	APPROVAL DATE	EFFECTIVE DATE
Mead Employees Credit Union Atlanta	MECU	03-03-2017	04-01-2017
First Intercontinental Bank Doraville	First IC Bank	04-05-2017	04-10-2017

FINANCIAL INSTITUTION MERGERS

FINANCIAL INSTITUTION (SURVIVOR)	MERGED INSTITUTION	APPROVAL DATE	EFFECTIVE DATE
SRP Federal Credit Union North Augusta, SC	Richmond County Health Department Employees Credit Union Augusta, GA	04-11-2017	

DBF Outreach
AND UPCOMING SPEAKING ENGAGEMENTS

Georgia Credit Union Affiliates 2017 Annual Convention -
Commissioner Kevin Hagler will be speaking at the GCUA 2017 Annual Convention in Savannah on Friday, May 19. For more information about this event visit http://www.gcuaforum.org/ac17/#!home.

The Department is the state agency that regulates and examines Georgia state-chartered banks, state-chartered credit unions, state-chartered trust companies, and bank holding companies that own Georgia state-chartered financial institutions. The Department also has responsibility for the supervision, regulation, and examination of Merchant Acquirer Limited Purpose Banks chartered in Georgia.

In addition, the Department has regulatory and/or licensing authority over mortgage brokers, lenders and processors, mortgage loan originators, check cashers, sellers-issuers of payment instruments, money transmitters, and international banking organizations.

Our **Mission** is to promote safe, sound, competitive financial services in Georgia through innovative, responsive regulation and supervision.

Our **Vision** is to be a willing and able partner with our regulated entities in order to support vibrant economic growth and prosperity in Georgia.

Subscribe to Receive this Publication:

This publication is delivered to interested parties via e-mail and is also available from the Department's website at http://dbf.georgia.gov/ under **Publications, Financial Institutions Bulletin**. To subscribe to this publication, please visit https://bkgfin.dbf.state.ga.us/GovDelivery.html.

Department of Banking and Finance
2990 Brandywine Road, Suite 200
Atlanta, Georgia 30341-5565
Phone: (770) 986-1633
Fax: (770) 986-1654 or 1655
http://dbf.georgia.gov/